HIPAA Security Policies and Procedures
For the
Department for Employee Insurance

PURPOSE:

The Department for Employee Insurance ("DEI") sponsors and administers a group health plan (the Plan) for employees, pursuant to KRS 18A.225, and is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). On behalf of the Plan (or on behalf of DEI for administrative functions of the Plan), employees of DEI's workforce may have access to electronic protected health information ("EPHI") that is identifiable to an individual. HIPAA and its implementing regulations require procedures for reasonably anticipated threats and hazards to electronic security. The purpose of the HIPAA Security Policies and Procedures for DEI is to ensure DEI's compliance with HIPAA and any applicable regulations. It is DEI's policy to comply fully with HIPAA's requirements. To that end, all DEI's employees and business associates who have access to EPHI must comply with these policies and procedures.

No third party rights (including but not limited to rights of the Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these policies and procedures. DEI reserves the right to amend or change these policies and procedures at any time without notice. To the extent these policies and procedures establish requirements and obligations above and beyond those required by HIPAA, the policies and procedures shall be objective and shall not be binding upon DEI. These policies and procedures do not address requirements under other federal laws or under state laws.

DEFINITIONS:

Business Associate: "Business associate" means a person who on behalf of DEI, other than a member of DEI's workforce, performs or assists in the performance of the following: (1) claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management or repricing, or (2) any other function or activity regulated by the privacy regulations, or (3) an entity that provides, other than in the capacity as a member of the work force of the covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, or financial services for DEI.

Covered Entity: "Covered entity" means health plans, health care clearinghouses, and health care providers that transmit health information in electronic format and others with respect to ascertaining the compliance of the covered entities and the enforcement of the applicable requirements. For the purpose of these policies and procedures, "covered entity" means DEI.

Employee: "Employee" means all members of DEI's workforce such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of DEI pursuant to employment status or contract, whether or not they are paid by DEI. The term "employee" includes individuals who would be considered part of the workforce under HIPAA

Electronic Protected Health Information ("EPHI"): "EPHI" means electronic health information that is identifiable to an individual. The definition includes, but is not limited to, telephone voice response and fax back (that is a request for information from a computer made via voice or telephone keypad input, with a request for information returned as a fax), emails, and files transmitted electronically)

Security Incident: "Security incident" means, but is not limited to, any misuse of electronic data.

STANDARDS and the PLAN'S RESPONSIBILITY FOR EPHI:

I. Administrative Safeguards

A. Assign Security Responsibility

The Commissioner of DEI shall identify a security official who is responsible for the development and implementation of the required policies and procedures.

DEI's Security Official was appointed on February 2, 2006. The individual responsible for the development and implementation of the required policies and procedures is the branch manager of the Data Analysis Branch. The branch manager reports directly to the deputy commissioner of DEI. The Security Officer will work in conjunction with the Systems Management staff within the Personnel Cabinet in the development and maintenance of the HIPAA Security policies and procedures.

The Security Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their EPHI.
The Security Official is responsible for creating a process for individuals to lodge complaints about the Plan's security procedures and for creating a system for handling such complaints.

B. Training of Workstation Use

DEI shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes or the surroundings of a specific workstation or class of workstations that can access EPHI.

The Security Official shall train all staff regarding HIPAA Security requirements as it pertains to their specific job duties. The Security Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions with the Plan.

New employees will receive HIPAA Security training within thirty (30) days of the date of hire. Each employee must sign a Security Practice Statement of Confidentiality upon completion of training.

C. Workforce Security

DEI shall ensure that all members of its workforce have access to EPHI appropriate to the duties of the workforce member and to prevent those workforce members who should not have access to EPHI from obtaining access. DEI's workforce security shall include the following:

1. Authorization and/or Supervision

DEI shall implement procedures for the authorization and/or supervision of workforce members who work with EPHI or who work in location where it might be accessed.

Both the Group Health Insurance (GHI) database and the Premium Bill and Reconciliation (PB&R) database are protected by login IDs and passwords. The levels of access to EPHI range from read-only to complete system access with the ability to change specific individual's EPHI. Only select management staff determines user access levels which are then maintained via a security table within the database (Table Maintenance). The user ID and password are stored within Table Maintenance, which may be updated only by select management staff.

2. Workforce Clearance Procedure

DEI shall determine that a workforce member's access to EPHI is appropriate.

Management staff is responsible for determining the level or access granted to staff based on their job duties. Every employee of DEI will access EPHI at some level in their daily job functions.

3. Termination Procedures

DEI shall have a process for terminating access to EPHI when the employment of a workforce member ends or when it is determined that it is not appropriate for certain workforce members to have access to EPHI.

Upon termination, all user access is revoked immediately within Table Maintenance and System Management staff is notified to immediately revoke system-wide user access. All keys and security ID badges will be turned in to the immediate supervisor.

II. System Safeguards

A. Workstation Security

DEI shall have physical safeguards for all workstations that access EPHI, in order to restrict access to authorized users.

All workstations automatically lock-out after ten (10) minutes. All screens must not face an open door. DEI shall, on behalf of the Plan, ensure that the appropriate technical and physical safeguards to prevent EPHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls.

B. Security Management Process

DEI shall prevent, detect, contain, and correct security violations. The Security Management Process shall include the following:

1. Risk Analysis

Annually, DEI shall conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability of EPHI.

2. Risk Management

DEI shall implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.

DEI will conduct an updated risk analysis each February and August in order to determine its continued compliance with HIPAA. As part of DEI's risk management, DEI compiled these policies and procedures which outline all the requirements of the HIPAA Security Rule.

3. Sanction Policy

DEI shall apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures.

Sanctions for using or disclosing EPHI in violation of the HIPAA Security Policies and Procedures may be imposed against any employee, including but not limited to, termination of employment.

4. Information System Activity Review

DEI shall regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Quarterly assessments are completed by third party vendors.

C. Information Access Management

DEI shall implement policies and procedures for authorizing appropriate access to EPHI. The policies and procedures shall include the following:

1. Isolating Health Care Clearinghouse Functions

Currently, DEI does not contract with a Health Care Clearinghouse. This does not apply to DEI's operation.

2. Access Authorization

DEI shall implement policies and procedures for granting access to EPHI.

To prevent unauthorized access, all employees of DEI must provide a unique ID and password when logging into their computer for system wide access. This level of security is maintained by System Management. In addition, to log into the GHI and PB&R databases a second ID and password are required. This security is maintained via Table Maintenance.

3. Access Establishment and Modification

Based upon the entity's access authorization policies, DEI shall establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Initial user access is established by Management Staff upon initial hiring. User access levels are modified on an "as needed" basis when changes in job responsibilities necessitate such action.

D. Protection from Malicious Software

DEI shall address how it will implement procedures that will guard against and detect and report malicious software (e.g. viruses or a virus reminder).

Systems Management staff uses McAfee Virus Scan. This protects the SQL server and all workstations and it is updated every workday. DEI's systems are also protected by a firewall within the Personnel Cabinet as well as one provided by the Commonwealth Office of Technology. The firewall is a hardware/software application and it protects against any unauthorized access to out network. The firewall is monitored by a third party vendor.

E. Log-in Monitoring

DEI should address how it will implement procedures that will monitor log-in attempts and report any discrepancies.

After three invalid attempts to log-in to the network the user is locked out and must contact Systems Management staff to unlock the workstation. If the user cannot remember their password, Systems Management staff may re-set the password. Systems Management staff verifies the identity of the individual prior to resetting of the passwords.

F. Password Management

DEI shall determine what procedures it must establish for password creation, change and safeguarding. For example, establishing a policy prohibiting posting passwords on post-it notes on monitors.

Every individual that accesses the network must create a unique password. It must be eight characters or more in length, and must meet at least three of the following conditions: upper case, lower case, number or symbol. Users are required to change their password every thirty (30) days, and the user cannot repeat a password used within the last twelve 30-day cycles. Passwords must remain in effect at least one day. Users are advised that passwords are confidential and should not be shared with other staff. At least every two months Systems Management staff audit passwords to identify any weaknesses.

G. Security Incident Procedures

DEI shall implement policies and procedures to address security incidents.

DEI shall identify and respond to suspected or known security incidents. DEI shall mitigate to the extent practicable, the harmful effects of security incidents that are known to the covered entity and to document security incidents and their outcomes.

When a security incident or deficiency is identified within program language within GHI or PB&R, IDMS staff is notified immediately and corrections to the GHI or PB&R system are made. A system tracking log is utilized to track problems identified with GHI or PB&R and their resolutions.

III. Contingency Plan Safeguards

DEI shall establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI.

A. Data Backup Plan

DEI shall establish and implement procedures to create and maintain exact copies of EPHI.

All information stored in the GHI or PB&R databases are backed up nightly to tape. The tapes are sent to an offsite facility every Friday. Tape backups that are sent offsite weekly are stored there for three weeks. After a tape has been stored for three weeks it is re-used, thereby limiting backup to three weeks activity. The daily backup schedule may be altered in the event of additional work days being added to the work week. In addition to the daily tape backup, DEI also copies the GHI/PB&R databases to another server that is offsite, which is not the same location as the tape backups). Also, transaction log backups are completed throughout the work day so that in the event of a minor disruption that does not destroy hardware, we may restore to the last transaction log backup.

B. Disaster Recovery Plan

DEI shall establish procedures to restore any loss of data.

Tape backups and server backups are stored in two different locations offsite. We may utilize new hardware and restore using the backup server with loss of data limited to no more than one day's data. If the backup server was also destroyed we would utilize the offsite tape backup with a loss of data limited to no more than one week's data.

C. Emergency Mode Operation

An emergency operations plan only involves those critical business processes that must occur to protect the security of EPHI during and immediately after a crisis situation.

DEI shall establish procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

In case of an emergency, DEI may physically move to the location of the backup server where DEI will have access to the GHI and PB&R databases. In the event the alternate location was destroyed, DEI would install hardware in a new location and restore it using backup tapes.

D. Testing and Revision Procedure

DEI shall implement procedures for periodic testing and revision of contingency plans.

The Disaster Recovery Plan is audited annually.

E. Applications and Data Criticality Analysis

DEI shall assess the relative criticality of specific applications and data in support of other contingency plan components.

GHI and PB&R are the most critical systems within the Department for Employee Insurance.

F. Evaluation

DEI shall perform technical and non-technical evaluation of the components of its security safeguards.

Evaluation is completed via quarterly reports from third party vendor and an annual report from the Kentucky State Auditor.

IV. Business Associate Contracts and Other Arrangements

DEI shall permit a business associate to create, receive, maintain, or transmit EPHI on the its behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information in accordance with the other applicable provisions of the security rule.

A. Written Contract or Other Arrangement

DEI shall require the covered entity to document the satisfactory assurances that it has received from its business associate through a written contract or other arrangement that meets the applicable requirements of the security rule.

Business associates with which DEI contracts are Humana Insurance Company, Express Scripts, Inc., PricewaterhouseCoopers, IDMS, and The Medstat Group. Contracts with each of these entities specifically require full compliance with both HIPAA Privacy and HIPAA Security requirements.

V. Facility Access Controls and Safeguards

DEI shall implement policies and procedures to limit physical access to its electronic information system and the facility or facilities in which they are house, while ensuring that properly authorized access is allowed.

A. Contingency Operations

DEI shall establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency-mode operations plan.

In the event of a disaster or the need to operate in an emergency situation, System Management staff will be responsible for restoring lost data. Only staff previously authorized to access EPHI will participate in the restoration processes.

B. Facility Security Plan

DEI shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

DEI requires a code to be entered to gain access to the computer room.
The Personnel Cabinet is in the process of issuing swipe cards to all employees. Employees will need swipe cards to gain access to their designated floor.
All hallways and offices have locks. Keys are issued to employees for access.
There are cameras on the exterior of the building.

C. Access Control and Validation Procedures

DEI shall implement procedures based on a person's role or function to control and validate his or her access to facilities, including visitor controls and control of access to software programs for testing and revision.

Those individuals with access to GHI and PB&R are also granted access to software programs for testing and revision. Management staff determines the level of security as previously indicated.

D. Maintenance Records

DEI shall document repairs and modifications to the physical components of a facility that are related to security.

All repairs to workstations are completed by Systems Management staff.

VI. Device and Media Controls

DEI shall govern the facility's receipt and removal of hardware and electronic media that contains EPHI and the movement of these items into, out of, and within the facility.

A. Disposal

DEI shall address the final disposition of EPHI and/or the electronic media on which it is stored.

Systems Management staff runs Wipedisk three times on all hard drives before they are disposed of permanently. CD's are shredded and diskettes are manually destroyed.

B. Media Re-Use

DEI shall remove EPHI from electronic media before the media are made available for re-use.

System Management runs Wipedisk three times on all hard drives prior to their re-use. This is the standard recommended by the Department of Defense.

C. Accountability

DEI shall maintain a record of the movement of hardware and electronic media and any person responsible therefore.

System Management staff maintain a log of the location of all workstations.

D. Data Backup and Storage

DEI shall create a retrievable, exact copy of EPHI, when needed, before movement of equipment.

All information stored in the GHI or PB&R databases are backed up nightly to tape. The tapes are sent to an offsite facility every Friday. Tape backups that are sent offsite weekly are stored there for three weeks. After a tape has been stored for three weeks it is re-used, thereby limiting backup to three weeks activity. The daily backup schedule may be altered in the event of additional work days begin

added to the work week. In addition to the daily tape backup, DEI also copies the GHI/PB&R databases to another server that is offsite, which is not the same location as the tape backups). Also, transaction log backups are completed throughout the work day so that in the event of a minor disruption that does not destroy hardware, we may restore to the last transaction log backup.

VII. Access Controls

DEI shall have policies and procedures for electronic information systems that maintain EPHI to allow access only to persons or software that have been granted access rights.

A. Unique User Identification

DEI shall assign a unique name and/or number for identifying and tracking user identity.

Each user is assigned a unique user ID for system wide access. The ID must be used in conjunction with the password. The same user ID is used to access GHI and PB&R but a different password is required.

B. Emergency Access

DEI shall have procedures for obtaining necessary EPHI during an emergency

Emergency procedures do not differ from daily operation procedures.

C. Automatic Logoff

DEI shall have electronic procedures to terminate an electronic session after a pre-determined time of inactivity.

After ten (10) minutes of idle time a password-protected screen-saver appears on all computers within DEI. Staff is advised to lock their screen whenever they leave their workstation.

VIII. Audit Controls

DEI shall have in place hardware, software, and/or procedural mechanisms that record and examine activity in information system that store or use EPHI. To record activity, GHI/PB&R creates notes when a record is updated/changed.

IX. Integrity Controls

DEI shall protect EPHI from improper alteration or destruction.

System access is only granted to those individuals whose job duties require access to EPHI. Staff is trained on the proper use of EPHI.

A. Mechanism to Authenticate EPHI

DEI shall implement electronic mechanisms to corroborate the EPHI has not been altered or destroyed in an unauthorized manner.

Via Table Maintenance, only users with a valid ID and password may access EPHI. Therefore, only those authorized users may access and/or change EPHI.

B. Person or Entity Authentication

DEI shall verify that person or entity seeking access to EPHI is the one claimed.

Via Table Maintenance, only users with a valid ID and Password may access EPHI. Therefore, only those authorized users may access and/or change EPHI.

Identity authentication occurs at several levels: at network login, filenet login, and within each application (GHI or PB&R).

X. Transmission Security

DEI shall have security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

A. Integrity

DEI shall have security measures to ensure that EPHI is not improperly modified without detection until disposed of properly.

Entrust is used to transmit information via email and BeyondFTP has its own ID and password for transmission or files outside of DEI's network.

B. Encryption

DEI shall encrypt EPHI whenever it is deemed appropriate.

File transfer protocol transmissions are secured by BeyondFTP.
Staff within DEI utilizes Entrust when sending emails that contain EPHI.